

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of Rao et al.

Filing Date: Herewith

Attorney File No.: 14846-32

Entitled: SINGLE SIGN-ON AUTHENTICATION SYSTEM

Assistant Commissioner for Patents
Washington, D.C. 20231

PETITION TO MAKE SPECIAL UNDER 37 C.F.R. § 1.102

SIR:

It is requested that the above-captioned patent application, filed herewith, be granted Special status for accelerated examination. As set forth in MPEP § 708.02(VIII), such a petition requires: (1) that all claims be directed to a single invention; (2) a pre-examination search; (3) copies of the references identified in the search deemed most closely related to the claimed subject matter; (4) a detailed discussion pointing out with particularity how the claimed subject matter is patentable over the references; and (5) the fee set forth in 37 C.F.R. 1.17(h). As set forth in more detail below, Applicants have complied with each of these requirements and granting of this Petition is respectfully requested.

I. APPLICANT'S CLAIMED INVENTION

Applicants' claimed invention is directed to systems and methods for enabling a secure, single sign-on to a computer network that requires comparatively less complexity and overhead than conventional single sign-on methods. A single sign-on authentication system includes an authentication component that determines whether a user is authenticated, and, if it is determined that the user is authenticated, generates a connection request, the connection request including an identifier and entitlement information. The system also includes an interface component that receives the connection request from the authentication component. The interface component

compares the received identifier with an expected identifier. If they match, the interface component makes the entitlement information available to a server associated with the interface component. A method for enabling an authenticated user to connect to a server in a computer network includes receiving a connection request for an authenticated user, the connection request including an identifier and entitlement information; comparing the received identifier with an expected identifier; and, if they match, making the entitlement information available to the server.

The current application comprises three independent claims. Independent claim 1 is directed to a single sign-on authentication system. Independent claim 8 is directed to a method for enabling an authenticated user to connect to a server in a computer network. Independent claim 15 is directed to a computer-readable medium for storing instructions for carrying out the method steps of claim 8.

Should the Examiner determine that the claims are not directed to a single invention, Applicants will make an election without traverse according to established telephone-restriction practice. MPEP 708.02(VIII).

II. PRE-EXAMINATION SEARCH

A pre-examination search was performed by the professional search firm of Woolcott LLC (“Woolcott”) to locate the U.S. Patents and U.S. Patent Publications relevant to the inventive concept (the “Search”). Woolcott is located at 2001 Jefferson Davis Highway, Suite 411, Arlington, Virginia 22202, Tel: 800.223.9697, and has a web page address of <http://www.woolcott.com/index.html>.

Copies of Woolcott’s Search Report and the identified references are attached. As can be seen from the Search Report, the following classes and subclasses were searched.

Class	Subclasses
713	200, 201, 202

Woolcott pointed out four references deemed most closely related to the claimed subject matter:

- (1) U.S. Patent 5,241,594 (issued Aug. 31, 1993) to Kung;
- (2) U.S. Patent 5,560,008 (issued Sep. 24, 1996) to Johnson et al. (“Johnson”);

(3) U.S. Patent 6,253,327 (issued Sep. 26, 2001) to Zhang et al. ("Zhang"); and
(4) U.S. Patent 6,453,353 (issued Sep. 17, 2002) to Win et al. ("Win")
(collectively referred to herein as the "Relevant References"). Each of the Relevant
References is discussed in detail below.

Nothing in this Petition should be construed as an admission that any reference
identified in the Search or discussed herein is available as prior art to the above-captioned
application.

III. DETAILED DISCUSSION OF PATENTABILITY

The claimed subject matter of the above-captioned patent application is patentable
over the Relevant References. Applicants provide detailed discussion in this Section that
points out with particularity how the claimed subject matter is patentable over the
Relevant References.

A. U.S. PATENT 5,241,594 (ISSUED AUG. 31, 1993) TO KUNG

The subject matter of the above-captioned patent application is patentable over
Kung. Among other deficiencies, Kung does not disclose a single sign-on system in
which once a user has successfully signed on to a network, any computer system in the
network receiving a connection request need only verify that the connection request was
received from the sign-on component. If the connection request originated with the sign-
on component, then there is no need to again query the user for authentication
information and to authenticate the user.

Kung discloses a multiple logon procedure that comprises a firmware or software
routine that is used in the communication protocol of the system between a
communication software program on a user's computer and a network communication
software program on each of the other computers in the system. The invention employs a
secure transport layer protocol that permits secure file transfer between computers of the
distributed system. Thus, when a user desires to use a particular computer, such as a
remote database, for example, a request initiated by the user is processed by the multiple
logon procedure which accesses the stored file that contains the user ID codes and
encrypted passwords, accesses the remote computer, and then enters the user's ID code
and password for that computer. This is done automatically, and the process is

transparent to the user and other users of the system. In essence, the remote computer interacts with the multiple logon procedure and its user ID code and password file, the multiple logon procedure decrypts the encrypted password for the particular requested computer and logs the user onto that computer using the ID code and decrypted password. Each user logs onto the distributed computing system only a single time and allows the user to access all available computers connected to the network. The system includes having a central server on which the IDs and encrypted passwords are stored, and a distributed system where IDs and encrypted passwords are stored at each respective computer in the system. All IDs and encrypted passwords are stored on a single computer which controls access to the entire distributed and networked system. Once access is granted to a particular user, nonencrypted passwords are transmitted to the remote computers, since the server provides for control of the entire networked system.

Since Kung does not teach or suggest Applicants' claimed invention, Applicants' invention as claimed is patentable over Kung.

B. U.S. PATENT 5,560,008 (ISSUED SEP. 24, 1996) TO JOHNSON

The subject matter of the above-captioned patent application is patentable over Johnson. Among other deficiencies, Johnson does not disclose a single sign-on system in which once a user has successfully signed on to a network, any computer system in the network receiving a connection request need only verify that the connection request was received from the sign-on component. If the connection request originated with the sign-on component, then there is no need to again query the user for authentication information and to authenticate the user.

Johnson discloses a system and method which authenticates a user by sending a message from the user's machines to a remote machine, i.e., from the client to the server, to perform the authentication. Once the user becomes authenticated, it is not desirable to repeat the authentication operation. However, the server is not forced to remember indefinitely the authentication and authentication information. Instead, an image of the user on the server is created, and then reconstructed for each request that the user makes. A method is invoked that concisely represents all of the capabilities of the user on the server, saves this information, and then reconstitutes the image of the user on the server

each time that an authentication request is run on that server for that user. A message, called a request for service, is sent from the user client machine to the server remote machine whenever that service is needed on the remote machine. The request for service contains enough information to insure that the remote user is authorized to use the server and the set of credentials and capabilities the user is to have when using resources on the server machine. The server builds a set of credentials that represent all the interesting security facts about the remote user. This information includes the user ID, the group ID that the user is in, the group set of other group IDs that the user has access to, an account ID, the set of privileges of the user that allow the user to bypass the normal security restrictions on the system, etc. The server establishes all of the credentials for the user, and stores this information in a data structure called the credentials structure, and returns a small value (e.g., 64 bits) to the client machine where the user is running. This returned small value is referred to as the credentials identifier. After the credentials identifier is returned to the user, all the user has to do is to present the credentials identifier to the server in every request requiring authentication that is made of that server. The server utilizes the credentials identifier to reconstitute the set of credentials that are saved away for that user.

Since Johnson does not teach or suggest Applicants' claimed invention, Applicants' invention as claimed is patentable over Johnson.

C. U.S. PATENT 6,253,327 (ISSUED SEP. 26, 2001) TO ZHANG

The subject matter of the above-captioned patent application is patentable over Zhang. Among other deficiencies, Zhang does not disclose a single sign-on system in which once a user has successfully signed on to a network, any computer system in the network receiving a connection request need only verify that the connection request was received from the sign-on component. If the connection request originated with the sign-on component, then there is no need to again query the user for authentication information and to authenticate the user.

Zhang discloses a method and apparatus for providing single-step logon access for a subscriber to a differentiated computer network having more than one separate access area. In a method for single-step logon, a network gateway grants a subscriber

access to both one or more public network domains, such as the Internet, and one or more private domains, such as community of interest domains or intra-network domains, without requiring the subscriber to launch a separate logon application. Once the subscriber has completed a single step logon to the network interface, the service provider is able to provide the subscriber with simultaneous secure channel access to both public areas and secured private areas. A network gateway interface provides the capability to authenticate the subscriber, provide the subscriber with an IP address and negotiate a point-to-point protocol session with the subscriber's host, thereby eliminating the need to have the subscriber logon for public access and then logon for private area access.

Since Zhang does not teach or suggest Applicants' claimed invention, Applicants' invention as claimed is patentable over Zhang.

D. U.S. PATENT 6,453,353 (ISSUED SEP. 17, 2002) TO WIN

The subject matter of the above-captioned patent application is patentable over Win. Among other deficiencies, Win does not disclose a single sign-on system in which once a user has successfully signed on to a network, any computer system in the network receiving a connection request need only verify that the connection request was received from the sign-on component. If the connection request originated with the sign-on component, then there is no need to again query the user for authentication information and to authenticate the user.

Win discloses a method of controlling access to one or more Web resources stored on a Web server, comprising the steps of receiving information describing a user at the Web server, identifying, at a Web application server coupled to the Web server, a subset of the resources that the user is authorized to access, based on stored information describing one or more roles and one or more access rights of the user that are stored in association with user identifying information, communicating information defining the subset to the first server, and communicating to a client that is associated with the user, a Web page containing links to only those resources that the user is authorized to access based on the user's role within an enterprise that controls the resources.

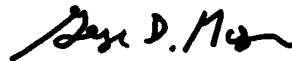
Since Win does not teach or suggest Applicants' claimed invention, Applicants' invention as claimed is patentable over Win.

Accordingly, because the Relevant References fail to teach or suggest one or more feature recited in the claimed subject matter, these references, either alone or in combination, would not have anticipated or rendered obvious the claimed subject matter.

IV. CONCLUSION

In view of the foregoing, Applicants' have met all the requirements for accelerated examination set forth in 37 C.F.R. § 1.102 and as detailed in MPEP § 708.02(VIII). Accordingly, Applicants respectfully request this case be made special for expedited examination. Please charge the required fee set forth in 37 C.F.R. § 1.17(h), estimated to be \$ 130.00, to Deposit Account No. 501358.

Respectfully submitted,



George D. Morgan
Reg. No. 46,505
Attorney for Applicant

November 24, 2003

LOWENSTEIN SANDLER PC
65 Livingston Avenue
Roseland, NJ 07068
Tel.: 973-597-6162

September 23, 2003

George D. Morgan, Esq.
Lowenstein Sandler PC
65 Livingston Avenue
Roseland, New Jersey 07068-1791

Re: Novelty Search "Single Sign-On Authentication System"

Your Ref: 14846-32

Our Ref: SANDLER-20053

Dear Mr. Morgan:

Further to your instructions of September 8, 2003, a novelty search has been conducted on the above identified subject matter

Objective:

The objective of the search is to locate references disclosing a single sign-on authentication system which includes an authentication component that determines whether a user is authenticated, and, if it is determined that the user is authenticated, generates a connection request, the connection request including an identifier and entitlement information. The system also includes an interface component that receives the connection request from the authentication component. The interface component compares the received identifier with an expected identifier. If they match, the interface component makes the entitlement information available to a server associated with the interface component.

Results of the Search:

Your attention is particularly directed to the following:

U.S. Patent Number 5,241,594 to Kung which discloses a multiple logon procedure that comprises a firmware or software routine that is used in the communication protocol of the system between a communication software program on a user's computer and a network communication software program on each of the other computers in the system. The present invention employs a secure transport layer protocol that permits secure file transfer between computers of the distributed system. Thus, when a user desires to use a particular computer, such as a remote database, for example, a request initiated by the user is processed by the multiple logon procedure

which accesses the stored file that contains the user ID codes and encrypted passwords, accesses the remote computer, and then enters the user's ID code and password for that computer. This is done automatically, and the process is transparent to the user and other users of the system. In essence, the remote computer interacts with the multiple logon procedure and its user ID code and password file, the multiple logon procedure decrypts the encrypted password for the particular requested computer and logs the user onto that computer using the ID code and decrypted password. Each user logs onto the distributed computing system only a single time and allows the user to access all available computers connected to the network. The system includes having a central server on which the IDs and encrypted passwords are stored, and a distributed system where IDs and encrypted passwords are stored at each respective computer in the system. All IDs and encrypted passwords are stored on a single computer which controls access to the entire distributed and networked system. Once access is granted to a particular user, nonencrypted passwords are transmitted to the remote computers, since the server provides for control of the entire networked system. Unique features of the distributed system of the present invention are that (1) the same password files are stored in all networked computers in the system, (2) once a user logs onto one computer, if the user wishes to use services at a second computer in the system, the authentication information is forwarded to the second computer by using a secure transport layer protocol for protecting its integrity, and (3) after it is received, the authentication information is compared with authentication information for the same user stored in the second computer. If the authentication information matches, the user is automatically logged onto the second computer. See column 3, line 14 – column 4, line 11.

U.S. Patent Number 5,560,008 to Johnson et al which discloses a system and method which authenticates a user by sending a message from the user machines to the remote machine, i.e., from the client to the server, to perform the authentication. Once the user becomes authenticated, it is not desirable to repeat the authentication operation. However, the server is not forced to remember indefinitely the authentication and authorization information. Instead, an image of the user on the server is created, and then reconstructed for each request that the user makes. A method is invoked that concisely represents all of the capabilities of the user on the server, saves this information, and then reconstitutes the image of the user on the server each time that an authentication request is run on that server for that user. A message, called a request for service, is sent from the user client machine to the server remote machine anytime that service is needed on the remote machine. The request for service contains enough information to insure that the remote user is authorized to use

the server and the set of credentials and capabilities the user is to have when using resources on the server machine. The server builds a set of credentials that represent all of the interesting security facts about the remote user. This information includes the user id, the group id that the user is in, the group set of other group ids that the user has access to, an account id, the set of privileges of the user that allow the user to bypass the normal security restrictions on the system, etc. The server establishes all of the credentials for the user, and stores this information in a data structure called the credentials structure, and returns a small value (e.g. 64 bits) to the client machine where the user is running. This returned small value is referred to as the credentials identifier. After the credentials identifier is returned to the user, all the user has to do is to present the credentials identifier to the server in every request requiring authentication that is made of that server. The server utilizes the credentials identifier to reconstitute the set of credentials that are saved away for that user. See column 5, line 34 - column 6, line 14.

U.S. Patent Number 6,253,327 to Zhang et al which discloses a method and apparatus for providing single-step logon access for a subscriber to a differentiated computer network having more than one separate access area. In a method for single-step logon a network gateway interface grants a subscriber access to both one or more public network domains, such as the Internet, and one or more private domains, such as community of interest domains or intra-network domains, without requiring the subscriber to launch a separate logon application. Once the subscriber has completed a single step logon to the network interface, the service provider is able to provide the subscriber with simultaneous secure channel access to both public areas and secured private areas. A network gateway interface provides the capability to authenticate the subscriber, provide the subscriber with an IP address and negotiate a point to point protocol session with the subscriber's host, thereby eliminating the need to have the subscriber logon for public area access and then logon for private area access. See column 4, lines 30 - 47.

U.S. Patent Number 6,453,353 to Win et al which discloses a method of controlling access to one or more Web resources stored on a Web server, comprising the steps of receiving information describing a user at the Web server; identifying, at a Web application server coupled to the Web server, a subset of the resources that the user is authorized to access, based on stored information describing one or more roles and one or more access rights of the user that are stored in association with user identifying information; communicating information defining the subset to the first server; and communicating, to a client that is associated with the user, a Web page

containing links to only those resources that the user is authorized to access, based on the user's role within an enterprise that controls the resources. See column 2, lines 44 - 56.

The following references have been found as being of interest:

<u>Patent Number</u>	<u>Inventor</u>	<u>Issue Date</u>
5,590,199	Krajewski et al.	12/31/1996
5,604,490	Blakely III et al.	02/18/1997
5,790,785	Klug et al.	08/04/1998
5,818,936	Moshayekhi	10/06/1998
5,944,824	He	08/31/1999
6,000,033	Kelly et al.	12/07/1999
6,092,196	Reiche	07/18/2000
6,178,511	Cohen et al.	01/23/2001
6,182,142	Win et al.	01/30/2001
6,182,225	Hagiuda et al.	01/30/2001
6,226,679	Gupta	05/01/2001
6,243,816	Fang et al.	06/05/2001
6,253,328	Smith Jr.	06/26/2001
6,275,944	Kao et al.	08/14/2001
6,308,273	Goertzel et al.	10/23/2001
6,311,275	Jin et al.	10/30/2001
6,317,838	Baize	11/13/2001
6,332,192	Boroditsky et al.	12/18/2001
6,401,211	Bresak Jr. Et al.	06/04/2002
6,408,389	Grawrock et al.	06/18/2002
6,460,141	Olden	10/01/2002
6,496,855	Hunt et al.	12/17/2002
6,496,936	French et al.	12/17/2002
6,510,523	Perlman et al	01/21/2003
6,535,917	Zamanzadeh et al.	03/18/2003
6,609,198	Wood et al.	08/19/2003
6,618,806	Brown et al.	09/09/2003
20020007460	Azuma	01/17/2002
20020104006	Boate et al..	08/01/2002

20020184507	Makower et al.	12/05/2002
20020188869	Patrick	12/12/2002
20030023880	Edward et al.	01/30/2003
20030046589	Gregg	03/06/2003
20030070069	Belapurkar et al.	04/10/2003
20030074580	Knouse et al.	04/17/2003
20030079147	Hsieh et al.	04/24/2003
20030084345	Bjornestad et al	03/01/2003
20030105981	Miller et al.	06/05/2003
20030159072	Bellinger et al.	08/21/2003
20030163733	Barriga-Caceres et al.	08/28/2003

The following nonpatent literature references have been found of interest:

www.dataviz.com/products/passwordplus, DataViz Password Plus software
www.thridmillennium.com, Key Minder software home page
<http://avirbin.com/passport.html>, Risks of the Passport Single Signon Protocol
<http://rhodessw.dezines.com>, AccountLogon
<http://www.entrust.com/entelligence/desktop/quicktour2.htm>

Title Temporary Global Passwords; Publication Date March, 1993

Title Method of Protecting Data on a Personal Computer; Publication Date November, 1985

Title Safe Single -Sign- On Protocol with Minimal Password Exposure No-Decryption, and Technology-Adaptivity; Publication Date March, 1995

Title Servlet/Applet/HTML Authentication Process with Single Sign- On
Publication Date January, 2000

"http://www.usenix.org/publications/library/proceedings/lis-ant98/full_papers/limoncelli/limoncelli_html/node16.html"; No "single log on" yet

<http://www.pcworld.com/resource/printable/article/0,aid,63244,00.asp>; Pondering Passport: Do You Trust Microsoft With Your Data?

George D. Morgan, Esq.
September 23, 2003
Page six

The field of search was directed to the following areas:

<u>Class</u>	<u>Subclasses</u>
713	200, 201, 202

Also, search nonpatent literature on Google, SPI.org, ieee.explore etc.

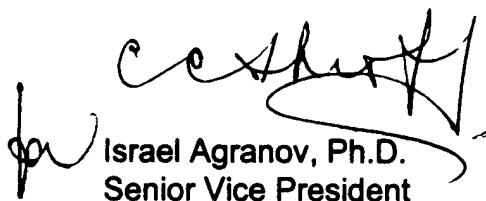
Examiner Allen Wu in art unit 2131 was consulted regarding the areas of search in class 713

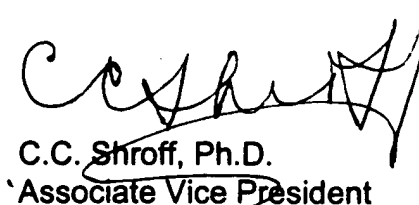
One set of references is enclosed and your disclosure is returned.

If we may be of any further service, please advise.

Thank you for giving us an opportunity to be of service to you.

Very truly yours,


Israel Agranov, Ph.D.
Senior Vice President


C.C. Shroff, Ph.D.
Associate Vice President

IA/CC/RR/ss

Enclosures